

NAVAL WAR COLLEGE
Newport, R.I.

Joint Vision 2010: Information Superiority and Its Effect on the Command and Control Process

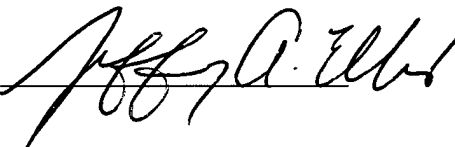
by

Jeffrey A. Ellis
Major, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

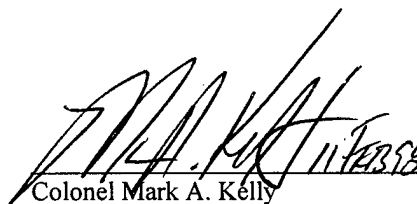
The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature



13 February 1998

Paper directed by Captain George Jackson
Chairman, Joint Military Operations Department



Colonel Mark A. Kelly
Faculty Advisor

19980708 056

DTIC QUALITY INSPECTED 1

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): Joint Vision 2010: Information Superiority and Its Effects on the Command and Control Process. (U)			
9. Personal Authors: Jeffrey A. Ellis, Major, USA			
10. Type of Report: FINAL		11. Date of Report: 13 Feb 1998	
12. Page Count: 19			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten Key Words That Relate To Your Paper: Joint Vision 2010, Information Superiority, Intelligence, Command and Control, Communications, Information, Decision-Making Process.			
15. Abstract: With the implementation of Joint Vision 2010, information superiority will impact every aspect of operational art, but none will be so great as the impact on operational command and control. Through information superiority, the operational commander theoretically gains a clearer picture of the battlespace, thus mitigating the fog of war. This study examines some of the potential command and control issues facing the operational commander as he attempts to conduct Major Operations and Campaigns. Given the diverse threat, it is doubtful that U.S. forces can gain and maintain information superiority over our enemies. The need for information superiority will hamper our ability to operate in a combined environment. Information superiority may lead to operational command and control that is too rigid and too centralized to maintain friendly freedom of action. Operational commanders may become transfixed by increasing levels of information focusing on data instead of the application of forces in space and time. In the end, information superiority will provide a clearer picture of the battlespace but it will not mitigate the fog of war.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Abstract of

Joint Vision 2010: Information Superiority and Its Effect on the Command and Control Process

With the implementation of Joint Vision 2010, information superiority will impact every aspect of operational art, but none will be so great as the impact on operational command and control. Through information superiority, the operational commander theoretically gains a clearer picture of the battlespace, thus mitigating the fog of war. This study examines some of the potential command and control issues facing the operational commander as he attempts to conduct Major Operations and Campaigns. Given the diverse threat, it is doubtful that U.S. forces can gain and maintain information superiority over our enemies. The need for information superiority will hamper our ability to operate in a combined environment. Information superiority may lead to operational command and control that is too rigid and too centralized to maintain friendly freedom of action. Operational commanders may become transfixed by increasing levels of information focusing on data instead of the application of forces in space and time. In the end, information superiority will provide a clearer picture of the battlespace but it will not mitigate the fog of war.

Introduction

In July of 1996, then Chairman of the Joint Chiefs of Staff, General John Shalikashvili released Joint Vision 2010. The publication provides "an operational template for the evolution of the Armed Forces for a challenging and uncertain future." One key aspect of Joint Vision 2010 is the introduction of the concept of information superiority. With the implementation of Joint Vision 2010, information superiority will impact every aspect of operational art, but none will be so great as the impact on operational command and control. Through information superiority, the operational commander theoretically gains a clearer picture of the battlespace, thus mitigating the fog of war. Unfortunately, certain aspects of information superiority warrant further investigation. It is doubtful that U.S. forces can gain and maintain information superiority over our enemies. The need for information superiority will hamper our ability to operate in a combined environment. Information superiority may lead to operational command and control that is too rigid and too centralized to maintain friendly freedom of action. Operational commanders may become transfixed by increasing levels of information focusing on data instead of the application of forces in space and time. In the end, information superiority will provide a clearer picture of the battlespace but it will not mitigate the fog of war.

It is extremely difficult if not nearly impossible to predict the future. Unfortunately, it also impossible to truly know how effective warfighting doctrine and concepts are until tested in battle against an enemy. Certainly no two improvements in command and control systems have effected the command and control process in the same manner; however, certain insights can be drawn between current trends such as the creation of information superiority as a doctrinal concept and those improvements in information processing data of the past such as the invention of the telephone. Joint Vision 2010 postulates that gathering, exploiting, and protecting information have been critical to command, control, and intelligence throughout

history and this will not change in the year 2010. Instead, what will change is access to information brought about by improvements in the speed and accuracy in transferring data.¹

What Is Information Superiority and Why Do Many Believe It Is So Critical To Future Success?

Command and control and the systems used in the process have undergone significant change in the last decade. Increasing levels of technology have produced faster, more capable command and control systems. In fact, technological advances have changed the way many think about the command and control process. Within the span of a few years, command and control expanded to include command, control, communications, computers, and intelligence. Systems designed to support command and control have evolved from fairly simple communications systems into complex information systems. Information and the ability to effectively handle it have taken center stage in virtually every aspect of military operations. Joint Vision 2010 not only recognizes the importance of information to operations; it mandates that United States forces control the flow of both friendly and enemy information on the battlefield. This condition will be known as information superiority. Joint Vision 2010 defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."² If truly achieved, information superiority will provide dramatic advantages in command and control over our enemies.

Information superiority will harness improvements in information and systems integration technology and build a "system of systems." This in turn will provide the commander with "dominant battlespace awareness, an interactive "picture" which will yield much more accurate assessments of friendly and enemy operations within the area of interest."³ The effects of information superiority are so great that four new operational concepts will be

¹U.S. Joint Chiefs of Staff. Joint Vision 2010 (Washington D.C. July 1996), 16.

²Joint Vision 2010, 16.

³Joint Vision 2010, 13.

born. They are: dominant maneuver, precision engagement, full dimensional protection, and focused logistics.⁴ Information superiority, not just intelligence or adequate command and control, will determine our ability to maneuver, engage the enemy in deep operations, and perform logistics operations.

During the Persian Gulf War, United States and Coalition forces achieved a degree of information superiority over Iraq. Coalition forces deprived the Iraqis their command and control communications, as well as their ability to collect intelligence through intelligence networks. At the same time, Coalition forces enjoyed effective command, control, and communications, as well as timely, accurate intelligence about the Iraqi forces.

It Is Doubtful That United States Forces Can Gain And Maintain Information Superiority Over Our Adversaries.

Generally speaking, when one thinks of superiority in warfare, it must be in relation to an enemy force, and more importantly, it must be in relation to an enemy force in terms of space and time. Both sea and air superiority are defined as, "That degree of dominance (in the air or at sea) of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force."⁵ How does the commander know when he has achieved information superiority if it does not have to relate to the enemy in terms of space and time? Suppose that U.S. forces are able to collect, process, and disseminate an uninterrupted flow of information in and across the theater of operations, but are unable to deny the enemy's capability to do the same. Does this mean they have failed to achieve information superiority?

No written documentation exists that discusses information superiority in the same terms as sea and air superiority, nor is there an expectation that United States can always expect to achieve information superiority. However, the unusually heavy emphasis on

⁴Joint Vision 2010, 19.

⁵U.S. Joint Chiefs of Staff. Department of Defense Dictionary, Joint Electronic Library (Joint Pub 1-02) (Washington D.C.: March 23, 1994), 30, 472

technology in Joint Vision 2010 and Expanding Joint Vision 2010 may cause one to infer that information superiority is the natural result of fielding technologically superior equipment. For instance, Joint Vision 2010 states: "technologically superior equipment has been critical to the success of our forces in combat,"⁶ and "...in all operations, technological advances will give our warfighters at the individual, crew, and small unit levels major qualitative advantages over our potential adversaries. Our forces will be able to sense dangers sooner. They will have increased awareness of the overall operational environment, including the situation of friendly forces, allowing them to make better decisions more rapidly."⁷ Expanding Joint Vision 2010 says that superior technology has been a cornerstone of the U.S. National Military Strategy since the dawn of the Cold War and will remain so through the year 2010."⁸

Warfare is not as simple as having the best command and control systems, and ironically, technological advances in command and control systems are often short lived. Worse, even when advantages are present, they may not yield much in the way of comparative advantage in a war.⁹ Such was the case during the Battle of the Atlantic in World War II. Both the Allies and the Germans attempted to gain an advantage over the other by either encrypting their own command and control messages or by attempting to decrypt their adversary's messages. Each side often intercepted and decoded each others messages and thus randomized tactical interplay, but instead of either side achieving any form of dominance over the other, the result was much like it would have been if no command and control systems were used at all.¹⁰

The information systems commanders will use to achieve information superiority are subject to a variety of threats. It is probable that potential adversaries understand our

⁶Joint Vision 2010, 7.

⁷Joint Vision 2010, 18.

⁸Expanding Joint Vision 2010, 24.

⁹Roger Beaumont, The Nerves of War: Emerging Issues in and References to Command and Control (Washington D.C.: AFCEA International Press, 1986), 56.

¹⁰Beaumont, 56.

dependence upon the information systems which carry command and control communications, intelligence, and logistical information. Increasing dependency on high technology command and control of military forces offers even greater rewards to an enemy who learns to mirror, spoof, or otherwise penetrate such systems.¹¹

The absence of the former Soviet Union as a principal adversary does not mean there is no longer a credible threat. Lieutenant General Otto Guenther, former Director of Information Systems for Command, Control, Communications, and Computers in the Office of the Secretary of the Army, described the threat as follows:

“It can be said that at the same time the Army was going through its “information revolution,” there was a parallel “threat revolution” occurring. This threat is constantly growing and is multifaceted. It comes from foreign governments (both enemy and ‘friendly’), drug cartels, terrorist organizations and individuals (from the curious intruder to the malicious hacker).”¹²

An alarming array of weapons is available for potential enemies to use in attacking our information systems. New technologies have revived old methods of espionage. Steganography, the practice of hiding messages within other messages, has found new life in the computer age. Computer technology applications for steganography allow hiding large data files inside digital graphic or audio files. It is possible to change a particular bit pattern in a graphics or sound file that alters the overt file, but does not change it in a way significant enough to arouse suspicion. Blank spaces in executable file patterns can be altered or used to activate other files such as extremely damaging viruses. To make matters worse, computer based steganography programs are available on nearly 60 web-sites on the Internet, yet there are currently no programs available to detect stenography.¹³ One does not have to be a Computer Scientist to see the utility of steganography for the enemy. Classified or highly

¹¹Beaumont, 55.

¹²Otto J. Guenther, “Managing the Race for Information Dominance,” *Army Magazine*, June 1997, 25.

¹³Clarence Hoop, “Steganography, Threat on the Internet: New Technologies Create New Opportunities for Hiding Messages,” 2 October 1997, <http://www.disa.mil/ciss/oct2.html#Steg/> (3 Dec 1997).

sensitive information could be stolen from our systems, viruses could be injected on our computer systems, or the operational characteristics of our systems could be changed without our knowledge.

Dependence upon information superiority subjects U.S. forces to the risk of defeat because of a single point of failure. As previously mentioned, each new tenant of Joint Vision 2010 requires information superiority for success. Together, the new operational tenants will allow the commander to achieve full spectrum dominance, but this cannot be achieved without information superiority. This brings into question reliability standards for command and control systems. Suppose that during an operation an information systems network had an operational readiness rate of 95%; any given system within the joint network could be expected to be non-operational for one hour and twenty minutes in a twenty-four hour day. It is a very remote possibility that all of the information systems within a joint network would fail at the same time; however, imagine the consequences if that happened. How would the commander conduct the campaign or major operation? United States forces would find themselves in a position much like the Iraqis did during the Gulf War.

As critical as information is to operational success, it is remarkable how little U. S. Military officers think in terms of losing their own communications. In 1991, a survey of U. S. Army War College Officers revealed that senior military leaders rarely think about the consequences of losing friendly communications. Senior officers gave little thought to communications during exercises and other types of simulated conflicts. The officers expected communications to be in place, operational, and reliable. When asked if their strategic, operational, or tactical decisions might be different if certain types of communications or services were interrupted or unavailable, every officer replied that they would be.¹⁴ While the

¹⁴Richard A. Muirragui, "Communications, The Forgotten Element of C³I: A Study of Wargaming, Modeling, and Simulations," USAWC Military Studies Program Paper, June 1991, 18.

survey only addressed exercise and simulation events, it is unlikely that these officers would have a different view during the initial phases of a conflict.

The Need For Information Superiority Will Adversely Impact Operational Command And Control In Combined Operations.

Both alliance and coalition warfare considerations will present major challenges for the commander under Joint Vision 2010; but coalition considerations will present the most obstacles to overcome. By its very nature, coalition warfare is highly turbulent. Coalitions usually lack common doctrine, compatible equipment, and common language. Coalition membership is usually of short duration, and unlike alliance warfare, there is little time to establish standards. Moreover, a nation that is our enemy today, may be our coalition partner tomorrow, or worse a nation that is our coalition partner today may be our enemy tomorrow. Recent history provides several examples of this trend. During the Gulf War, the United States went to war with Iraq, a nation that it supported during the war between Iran and Iraq. Several Warsaw Pact nations also participated in the Coalition against Iraq.

Intelligence sharing is one of the greatest problems associated with coalition warfare. Sharing intelligence may expose United States collection and analysis capabilities to a future enemy. This may jeopardize future military operations, risk American lives, and ultimately endanger the security of the nation. On the other hand, if commanders do not share vital intelligence, their immediate operations may fail. Further, refusal to share intelligence with coalition partners may cause them to refuse intelligence to the United States. Overall, this could effect the ability to obtain information superiority. In 1993, General Robert Risscassi, then Commander in Chief of the United Nations and Republic of Korea-United States Combined Command, and Commander United States Forces, Korea described the delicate intelligence balance as follows:

“The United States brings to battle the most sophisticated and enviable capability to gain deep operations visibility of any nation in the world. If it is kept in seclusion, it will significantly reduce the combat power available for deep

operations and force other alliance members to fight blindly with regard to time.... Yet few nations, including the United States are willing to share the sensitive sources of intelligence gathering or enlighten other nations on the technical strengths and weaknesses of various collection means.”¹⁵

The issues involved with intelligence sharing are serious; the decision to withhold intelligence will limit our ability to fight in an ad hoc coalition and simultaneously achieve information superiority. Unfortunately, this is not the only issue associated with achieving information superiority in combined operations.

United States forces will lose flexibility with both our long standing allies and potential ad hoc coalition partners in terms of systems and doctrinal interoperability. The ability to communicate and share information both vertically and horizontally is critical to success across the battlespace. Unfortunately, the technical systems required to achieve information superiority may outpace our allies or partners. Equipment incompatibility will result in the inability to communicate or share other information with either our allies or coalition partners.

“Applying the tenants of combined doctrine relies on a command, control, communications, computers, and intelligence architecture that is capable of integrating the joint forces of all nations in the coalition. It is in the various functions embedded in C⁴I that American forces possess some of their greatest advantages on the battlefield. Indeed, as we continue to improve our capabilities for collecting, analyzing, and disseminating intelligence, managing the vast amounts of information upon which decisions are made and incorporating more and more computer aids to the battlefield decision and execution processes, we must exercise care that these systems do not evolve into exclusionary processes. Unless the architecture incorporates the ability to share with, and in turn receive from, other national forces, the battlefield will not be seamless and significant risks will be present.”¹⁶

Even simple differences found in combined warfare such as languages are bound to have an effect on information superiority. Combat directives must be translated and distributed to each partner of the coalition in a language that they understand. With each translation, there is

¹⁵Robert W. Risscassi, “Principles for Coalition Warfare,” *Joint Force Quarterly*, Summer 1993, 70.

¹⁶Risscassi, 69.

a potential for error; moreover, each translation takes valuable time¹⁷. Errors and long processing times hamper or even prevent the uninterrupted flow of information to and from our allies and coalition partners. This in turn negates any advantage achieved through information superiority, or worse, precludes achieving information security.

Not every ally or potential coalition partner will share our view of future military operations, nor will they necessarily adopt doctrine similar to that of Joint Vision 2010. Over time, this will affect our ability to integrate combat actions with other nations. Once United States forces adopt, train with, and become accustomed to operating with information superiority, they will lose their ability to operate without it. This will doctrinally separate our forces from all other nations. The absence of a common doctrine generally results in the severe narrowing in the amount of information conveyed between coalition commanders.¹⁸ This will ultimately degrade our performance as information superiority depends upon the ability to maintain an unrestricted flow of information.

Consider the following scenario: U.S. forces become involved in a combined operation as a member of a coalition. The commander may not be able to talk with, relay orders to, exchange intelligence with, or synchronize combat actions with units to his right or left if they are not a part of the United States military. It is easy to visualize weak areas within the battlespace that could be easily exploited by an adversary who understands Joint Vision 2010 and United States dependence upon information superiority.

Operational Command And Control May Become Too Rigid And Too Centralized.

The American military depends upon centralized planning and decentralized execution for success. Commanders and leaders at every level encourage subordinates to use initiative and make decisions. Bold risk takers who act prudently are characteristically rewarded. Understanding the commander's intent is key to this method of war fighting; if a subordinate

¹⁷Risscassi, 69.

¹⁸Risscassi, 69.

knows what his commander expects or intends to do, he can make the correct decision when confronted with a situation where the commander is absent and an immediate decision is needed. Increases in the flow of information achieved through information superiority should eliminate some of the situations which force subordinates to make these decisions. Through information superiority, commanders should have an unprecedented awareness of the overall battlefield situation, as well as, the situations faced by their subordinates. It is natural to expect this will lead to better decisions by commanders at every level; however, this is not necessarily the case. Training with reduced command information capabilities in some cases may prove as, or even more valuable than, investing in advanced technologies.¹⁹

Situational awareness may also lead to a mindset that causes commanders to feel less inclined to articulate their intent or to issue mission-type orders. "Increasingly capable C⁴ systems... encourage commanders to feel that there is less need either for flexible orders or the intensive planning that produced them. Thus, modern C⁴ systems instead of enhancing the classic military process, seem to have become a substitute for it."²⁰

In the past, the increased ability to gather information about the actions of subordinate units did not result in better decisions nor did it have a remarkable impact upon the outcome of operations. During World War I, armies of the world experienced a technical revolution in communications not unlike the computer age of today. Almost overnight, commanders could communicate with their subordinates without being physically present in every location. Both the British and German command systems became more centralized as commanders were able to more quickly gain increased levels of information about from subordinates. Even German Army commanders and their staffs, masters of the use of commander's intent and mission-type

¹⁹Beaumont, 55.

²⁰Frank M. Snyder, Command and Control, The Literature and Commentaries (Washington D.C. National Defense University, 1993), 61.

orders, "fell victim to telephonitis, a tendency by higher headquarters to interfere in every small detail simply because it was so easily done."²¹

Operational Commanders May Become Transfixed By Increasing Levels Of Information Focusing On Data Instead Of The Application Of Forces In Space And Time.

When making decisions, commanders seek information in order to reduce uncertainty and make the best decision possible. Knowledge about a given situation enables them to formulate and choose courses of action that have a greater chance of success or achieve their desired results with a minimum amount of casualties. Increased amounts of information may enable a commander to make better or faster decisions than the enemy, once again increasing our chances of success or minimizing injury or loss of life. However, like every other aspect of military art, too much of a good thing is a recipe for disaster. Too much information may hinder the command and control process. Consequently, commanders may become transfixed by data, losing sight of its purpose, and thereby decreasing the speed with which decisions are made.

By the year 2010, U.S. Commanders will have an unprecedented amount of intelligence information to aid in the decision making process. Although some of this intelligence information will help the commander gain a better picture of the battlespace, much will add to the uncertainty that surrounds the decision making process. Over 100 years ago, Carl Von Clausewitz wrote about intelligence and information, its effect on the commander's decisions, and ultimately command and control. According to Clausewitz,

"If we consider the actual basis of this information, how unreliable and transient it is, we soon realize that war is a flimsy structure that can easily collapse and bury us in its ruins...Many intelligence reports in war are contradictory; even more are false, and most are uncertain. What one can reasonably ask of an

²¹Martin Van Creveld, Command in War (Cambridge, Massachusetts and London, England, Harvard University Press, 1985), 169.

officer is that he should possess a standard of judgment, which he can gain only from the knowledge of his men and affairs and from common sense."²²

Much of Clausewitz's theory is still valid today. Many pieces of information received by the commander are contradictory and many may be false. Good judgment and a thorough understanding of the situation at hand are still necessary to sort out the sea of information that flows to the commander.

"To believe that the wars of the future, thanks to some extraordinary technological advances yet to take place in such fields as computers or remotely controlled sensors, will be less opaque and therefore more subject to rational calculations than their predecessors is, accordingly sheer delusion."²³

Given this reality, commanders must understand what information is critical and what information will simply overload their ability to decide. Simply having information superiority will not ensure that the commander will make the most appropriate use of the information he has. Further, commanders must never request or require data or information simply because they can. To do so may rob subordinates of their freedom of action by forcing them to focus on data instead of their warfighting tasks.

The tendency to demand more information and suffer from information overload may be more prevalent in Operations Other Than War or Counterinsurgency environments. In these settings, military success is often hard to define and even more difficult to quantify. This can greatly exacerbate the uncertainty that surrounds the decision-making process. As uncertainty increases, the demand for information rises. In such cases, much of the information gathered by commanders is not relevant to the decision-making process or the actual situation at hand. Such was the case during the Vietnam War. Due to the relatively stagnate nature of the battlefield, progress was virtually unobserved and to extremely difficult to measure. As the war progressed, political, social, and economic pressures mounted. In addition, most commanders

²²Carl Von Clausewitz, On War, Michael Howard and Peter Paret, ed. (Princeton, N.J.: Princeton University Press, 1984), 117.

²³Creveld, 266.

knew little about the nature of the war that they were fighting in Vietnam. Eventually, this led commanders and politicians to use statistics to measure the success of their military actions. Unfortunately, statistics, even when accurate, did not substitute for a working knowledge and understanding of the military environment; however, previously unprecedented increases in the capabilities of command and control systems enabled commanders and their staffs at every level to generate volumes of facts. The demand for information not related to combat decision making skyrocketed and leaders converted real political and military problems into bogus, technical ones.²⁴

The ability to collect greater levels of information does not necessarily translate into better decisions. One study of civilian managers noted that:

“Managers are susceptible to the myriad limitations of most human decision makers. Much evidence indicates that superficial information search and processing biases cause gross errors in human decision making. Decision makers: gather information and then don’t use it; ask for more information and tend to ignore it; often make decisions first and look for relevant information afterward; tend to gather a great deal of information that has little or no relevance to the decision-making situation at hand.”²⁵

A similar trend exists among military commanders. It is also noteworthy that military commanders often attempt to use improvements in information technology including faster information processing in an attempt to eliminate uncertainty in the decision making process. Unfortunately, increases in information technology throughout history have done little to alleviate uncertainty. It is unlikely that improvements in information system technologies will help eliminate uncertainty in the future.²⁶

Historically, the increased ability to process command and control information has not improved the quality of decision making; instead, it has merely generated a greater demand for

²⁴Crevel, 252-253.

²⁵E. Frank Harrison, The Managerial Decision-Making Process, 3rd ed. (Boston: Houghton Mifflin Co., 1987), 42.

²⁶Crevel, 265-266.

more information. During World War I, both German and Allied commanders and their staffs, were notorious for requiring increasing amounts of information from subordinate Commands, even though the information had no impact on the operations at hand. In Germany, the requirements for paperwork, forms, correspondence became so great, World War I was known as the der Papierkrieg, the Paper War.”²⁷

Conclusions

The concept of information superiority as described in Joint Vision 2010 and Expanding Joint Vision 2010 is somewhat inconsistent with other Joint doctrine. The failure to address information superiority in terms of time and space ignores the fundamental principles of operational art.

While it is true that U.S. and Coalition forces gained a degree of information superiority over Iraq during the Gulf War, few adversaries will allow that luxury in the future. United States forces will not gain and maintain a sufficient advantage over potential adversaries through information superiority. No nation has ever gained a significant advantage in war through technologically advanced information systems and it is unlikely the United States will achieve an advantage in the year 2010. It is reasonable to expect that future adversaries will understand the value of information superiority to U.S. forces. Commanders must expect attacks on friendly information systems in war. Information systems are extremely vulnerable to sabotage and attack. This coupled with the increase in the number of threats will pose a tremendous threat to gaining and maintaining information superiority.

Information superiority demands highly technical information systems and equipment. This coupled with the need to protect intelligence collection procedures and the dramatic changes in doctrine will greatly limit U.S. forces ability to conduct alliance and coalition warfare.

²⁷Creveld, 169.

Situational awareness is a double-edged sword. Commanders gain an increased knowledge of the battlespace, but human nature and past experience dictate that it comes at the expense of flexibility, planning, and initiative.

Information superiority cannot eliminate all uncertainty in the decision-making process, nor can it ever replace the value of the commander's judgment. Commanders will almost always want and receive too much information. For which a great deal will have no impact on the decision at hand. This will cause the timeliness of decisions to suffer.

Improvements in information systems technologies as well as improvements in intelligence sensors cannot eliminate uncertainty in the decision making process. This leads to the obvious conclusion that ultimately, information superiority cannot and will not mitigate the effects of the fog of war. Unfortunately, for every vapor of fog that it dissipates, another is created.

Recommendations

Joint Vision 2010 and the concept of information superiority must be reevaluated to address the reality that United States forces may not always be able to collect, process, and disseminate an uninterrupted flow of information. The concept should further reflect that United States forces may also fail to exploit or deny an adversary's from collecting, processing, and disseminating an uninterrupted flow of information across the battlespace. The concept of information superiority should more closely resemble the concepts of air and sea superiority allowing for varying degrees of domination over the enemy in space and time. Operational commanders must view information superiority as one more element of battle to be achieved through the application operational art; not a capability derived through technology.

Information systems security must be given a very high priority. Countermeasures to technologies such as computer steganography must be developed. Commanders must seriously address the vulnerability of their information systems and plan for their defense against a wide array of threats.

Doctrine must be developed for operating in a combined environment. It must address the issues of intelligence sharing and information dissemination. Further, serious consideration must be given to doctrinal as well as equipment interoperability. The United States must purchase equipment that can operate in a highly sophisticated network while interfacing with potentially less sophisticated allied or coalition equipment.

If information superiority brings a new way of looking at command and control, Commanders must understand what to expect. They must become aware of the impacts of technology, all impacts, not just the ability to see more of the battlespace. Commanders must also remain vigilant so that the military planning process is not replaced by tighter control. Limiting the ability of the commander to "reach down and touch a subordinate." may be wise. During peacetime, training should be conducted with restricted command and control information systems.

Developing procedures to determine the type and amount of information needed in the decision making process is necessary. Dividing the battlespace into belts or boxes, similar to the wargaming process performed in the Commander's Estimate process at the tactical level, may provide a method of managing the overwhelming volume of battlespace information. After thorough analysis, the commander could specify events or points in time to trigger the delivery of timely, relevant information, instead of receiving a constant flood of useless data.

BIBLIOGRAPHY

- Beaumont, Roger. The Nerves of War: Emerging Issues in and References to Command and Control. Washington D.C.: AFCEA International Press, 1986.
- Clausewitz, Carl. On War, Edited by Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1984.
- Creveld, Martin Van. Command in War. Cambridge, Massachusetts and London, England: Harvard University Press, 1985.
- Guenther, Otto J. "Managing the Race for Information Dominance," Army Magazine, June 1997.
- Harrison, Frank E. The Managerial Decision-Making Process. 3rd ed. Boston, Massachusetts: Houghton Mifflin Co., 1987.
- Hoop, Clarence, "Steganography, Threat on the Internet: New Technologies Create New Opportunities for Hiding Messages." 2 October 1997.
<http://www.disa.mil/ciss/oct2.html#Steg/> (3 Dec 1997).
- Muirragui, Richard A. "Communications the Forgotten Element of C3I: A Study of Wargaming, Modeling, and Simulations," USAWC Military Studies Program Paper. June 1991.
- Risscassi, Robert W. "Principles for Coalition Warfare," Joint Force Quarterly, Summer 1993.
- Snyder, Frank M. Command and Control, The Literature and Commentaries. Washington D.C.: National Defense University, 1993.
- U.S. Joint Chiefs of Staff. Department of Defense Dictionary, Joint Electronic Library (Joint Pub 1-02) Washington D.C.: March 23, 1994
- U.S. Joint Chiefs of Staff. Joint Vision 2010. Washington D.C. July 1996.
- U.S. Joint Chiefs of Staff. Concept for Future Joint Operations: Expanding Joint Vision 2010. Washington D.C.: May 1997.